verizon

# BLACKBERRY 10

## SECURITY GUIDE

CONFIDENTIALITY. INTEGRITY. AUTHENTICITY.

# CONTENTS


**BLACKBERRY 10 AND VERIZON 4G LTE** ..... 3

**THE VERIZON-BLACKBERRY SECURITY SOLUTION** ..... 5

**PROTECTING DATA IN MOTION** ..... 6

BLACKBERRY ENTERPRISE SERVICE 10 OVERVIEW ..... 6

BES10 SECURITY PHILOSOPHY ..... 7

BLACKBERRY 10/BES10 FIPS 140-2 CERTIFICATION ..... 7

*TECH CORNER 1*: FIPS 140-2 CERTIFICATION DETAILS ..... 7

ENCRYPTION OPTIONS ..... 8

S/MIME MESSAGING ENCRYPTION ..... 8

COMMON ACCESS CARD/SMART CARD READER SUPPORT ..... 8

BLACKBERRY SMART CARD READER ..... 8

*TECH CORNER 2*: S/MIME KEYS, CERTIFICATES AND ENCRYPTION ALGORITHMS ..... 8

BES10 LAYERS OF PROTECTION ..... 9

**PROTECTING DATA AT REST** ..... 10

BLACKBERRY BALANCE OVERVIEW AND FEATURES ..... 10

BUILT-IN PASSWORD PROTECTION ..... 11

BLACKBERRY BALANCE *IN ACTION* ..... 11

*TECH CORNER 3*: WORK PERIMETERS/PERSONAL PERIMETERS IN DETAIL ..... 11

**STRONG ACCESS CONTROLS** ..... 12

BLACKBERRY HARDWARE ROOT OF TRUST ..... 12

AUTHENTICATION ..... 13

BLACKBERRY DEVICE OS SECURITY FEATURES ..... 13

BLACKBERRY WORLD ..... 13

**ENTERPRISE MOBILITY** ..... 14

BLACKBERRY 10 DEVICE ACTIVATION ..... 14

BLACKBERRY USER AUTHENTICATION *IN ACTION* ..... 15

MANAGING DEVICES USING DEVICE WIPE ..... 15

DEVICE WIPE *IN ACTION* ..... 15

DISTRIBUTION AND APPLICATION SECURITY USING BLACKBERRY WORLD FOR WORK ..... 15

APPLICATION SANDBOXING ..... 16

MALWARE CONTROLS ..... 16

MALWARE PROTECTION *IN ACTION* ..... 16

**REGULATED COMPLIANCE** ..... 17

BES10 REGULATED FEATURES AND CAPABILITIES ..... 17

*TECH CORNER 4*: BES10 REGULATED WORK PERIMETER ..... 18

**GOVERNMENT: SECURING DATA AND PUBLIC TRUST** ..... 19

**HEALTHCARE: SECURING THE FLOW OF PROTECTED HEALTH DATA** ..... 20

**FINANCIAL SERVICES: MOBILITY IN A HIGHLY REGULATED ENVIRONMENT** ..... 21

**VERIZON AND BLACKBERRY: THE GOLD STANDARD FOR DATA PROTECTION** ..... 22

# BLACKBERRY 10 AND VERIZON 4G LTE: THE GOLD STANDARD FOR END-TO-END MOBILE DATA SECURITY

KEEPING MOBILE DATA SECURE IS A TOP PRIORITY FOR ANY ORGANIZATION. AFTER ALL, A DATA BREACH CAN CAUSE SIGNIFICANT FINANCIAL LOSSES, DAMAGE YOUR COMPANY'S REPUTATION AND WEAKEN OR ELIMINATE COMPETITIVE BUSINESS ADVANTAGES.

As more mobile employees access your corporate network to communicate, collaborate and share data, your infrastructure becomes more vulnerable to outside attacks and harder to secure and protect. The mixing of personal and work email accounts, files and data, as well as the proliferation of employee-owned devices, increases the chance of major data leaks.

**THE JOINT VERIZON-BLACKBERRY SOLUTION SECURES DATA FROM WOULD-BE ATTACKS AND LOSS.**

## CONSIDER THE FOLLOWING FACTS:*

**71%** OF SECURITY BREACHES **TARGETED USER DEVICES.**

**40%** OF ATTACKS **INCORPORATED MALWARE.**

**76%** OF NETWORK INTRUSIONS RESULTED **FROM EXPLOITED OR STOLEN CREDENTIALS.**

**52%** OF SUCCESSFUL ATTACKS **USED SOME FORM OF HACKING.**

**75%** OF BREACHES ARE CONSIDERED **OPPORTUNISTIC ATTACKS.**

**37%** OF BREACHES AFFECTED **FINANCIAL ORGANIZATIONS.**

**"...BREACHES ARE A MULTI-FACETED PROBLEM, AND ANY ONE-DIMENSIONAL ATTEMPT TO DESCRIBE THEM FAILS TO ADEQUATELY CAPTURE THEIR COMPLEXITY."**

***—2013 DATA BREACH INVESTIGATIONS REPORT***

IT managers must now consider a highly complex corporate network infrastructure when devising a plan to protect and secure corporate information.

The entryways for potential attacks include:

+ Employees co-mingling corporate and third-party applications on the same device.
+ Personal and corporate email accounts shared on the same device and employees exchanging information between the two.
+ Employees visiting sites where they encounter malware or malicious threats.
+ The use of employee-owned devices to access enterprise resources and information.

IT managers need a solution that helps them:

+ Deliver transparent security for an optimal user experience.
+ Provide integrated containerization that enables simple enterprise application development and deployment.
+ Reduce employee misuse of devices.
+ Keep personal and work information separate.
+ Ensure that the network transport and data at rest are kept secure.
+ Eliminate personal work spaces and fully control device hardware.

Together, Verizon and BlackBerry deliver a solution that satisfies the security needs of both enterprises and government agencies. This joint solution provides the confidentiality, integrity and authenticity to help protect your organization from data loss and theft while delivering a seamless and simple end-user experience.

***2013 Verizon Data Breach Investigations Report***

# THE VERIZON-BLACKBERRY SECURITY SOLUTION:

## A STRONG, SECURE NETWORK AND INFRASTRUCTURE FOR END-TO-END MOBILE DATA PROTECTION

**DATA TRANSMITTED FROM A MOBILE DEVICE IS ONLY AS SECURE AS THE NETWORK IT TRAVERSES. THAT'S WHY VERIZON HAS INVESTED MORE THAN $80 BILLION IN ITS INFRASTRUCTURE TO SECURE YOUR DATA AS IT TRAVELS OUR NETWORK. THE VERIZON 4G LTE NETWORK CONTAINS A NUMBER OF BUILT-IN SECURITY MEASURES, SUCH AS SECURE STORAGE, MUTUAL AUTHENTICATION, 128-BIT ENCRYPTION AND AIRLINK CIPHERING, TO KEEP DATA TRANSMISSIONS SAFE.**

The Verizon network, combined with BlackBerry's infrastructure authentication, device management capabilities and hardened BlackBerry® 10 operating system, offers the gold standard for end-to-end mobile security.

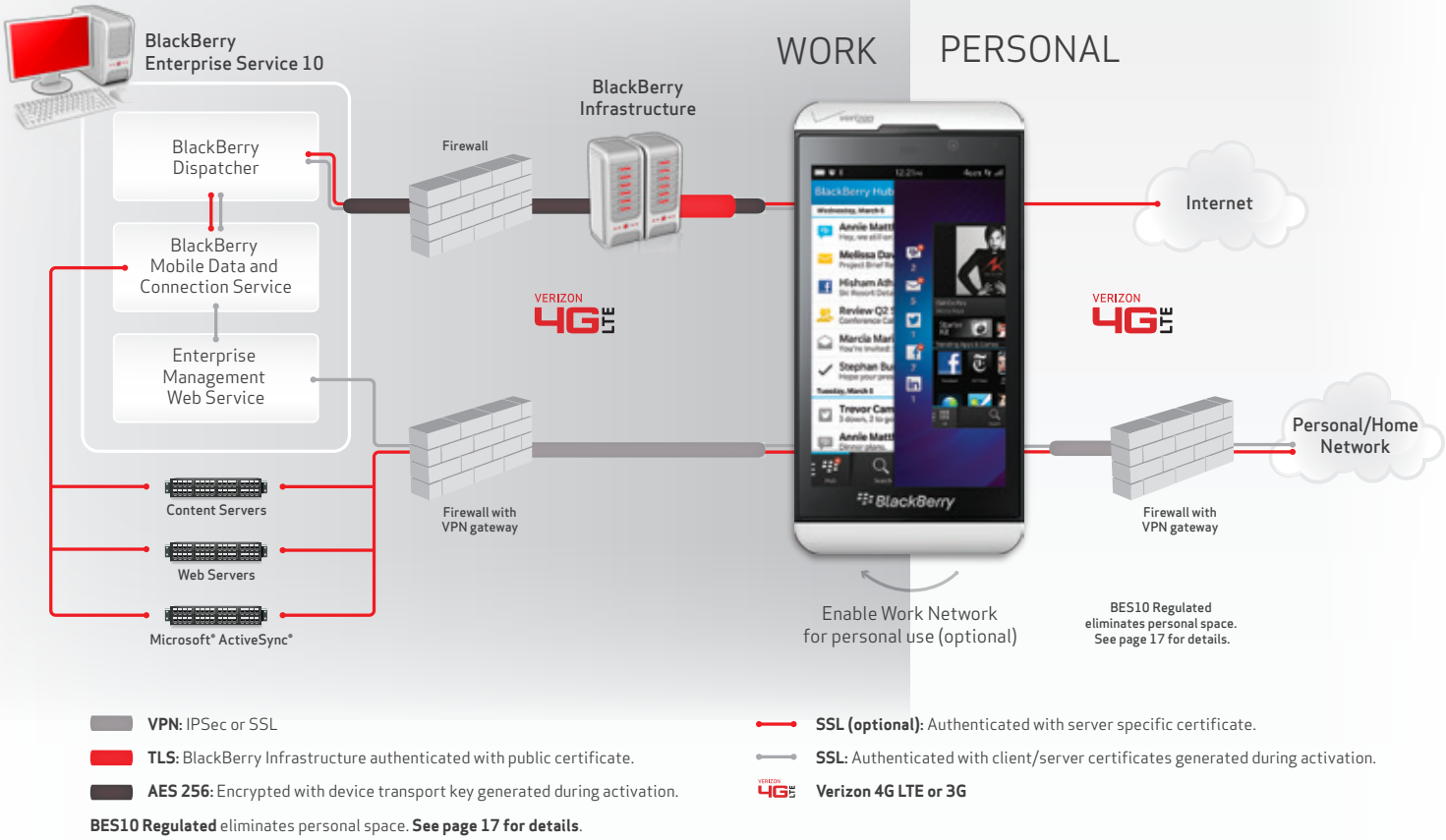
The Verizon-BlackBerry security solution focuses on five critical areas of protection:

1. PROTECTING DATA IN MOTION
2. PROTECTING DATA AT REST
3. STRONG ACCESS CONTROLS
4. ENTERPRISE MOBILITY MANAGEMENT
5. REGULATED COMPLIANCE

These five areas help protect your data from breaches, losses or alterations as it travels from your enterprise over the Verizon 4G LTE network to your employees' BlackBerry devices.

# PROTECTING DATA IN MOTION

## A KEY ELEMENT OF THE BLACKBERRY SOLUTION FOR IN-TRANSIT DATA SECURITY IS BLACKBERRY ENTERPRISE SERVICE 10.




BECAUSE MANY OF YOUR EMPLOYEES WORK OUTSIDE THE OFFICE, IT'S CRITICAL THAT YOU HAVE STRONG SECURITY MEASURES IN PLACE—BOTH ON EMPLOYEES' DEVICES AND INTERNAL NETWORK INFRASTRUCTURE—TO PROTECT DATA IN TRANSIT. A KEY ELEMENT OF THE BLACKBERRY SOLUTION FOR IN-TRANSIT DATA SECURITY IS BLACKBERRY ENTERPRISE SERVICE 10 (BES10). BES10, WITH ITS BUILT-IN DATA ENCRYPTION AND CERTIFICATION CAPABILITIES, HELPS BOTH ENTERPRISES AND GOVERNMENT AGENCIES PROTECT SENSITIVE INFORMATION AND MINIMIZE DATA LOSS OR ALTERATION.

## BLACKBERRY ENTERPRISE SERVICE 10 OVERVIEW

BES10 secures in-transit data using transport layer encryption and transport layer security (TLS) to encrypt it over the BlackBerry infrastructure. Before data transmission takes place, the data is compressed and encrypted, while the message keys are encrypted by the device transport key.

When data is received, the BES10 and the device both use the device transport key to decrypt the message keys and then decrypt and decompress the data.

## BES10 SECURITY PHILOSOPHY

The security features found in BES10 are built upon a foundation of confidentiality, integrity and authenticity:

+ **Confidentiality**: BES10 encryption helps ensure that only intended recipients can view email messages and prevents comingling of data across end users' corporate and personal applications.
+ **Integrity**: All email sent over the secure Verizon 4G LTE network are strongly encrypted to keep third parties from decrypting or altering the message.
+ **Authenticity:** Before data is delivered to a device, BES10 authenticates the device's transport key used to encrypt the data, helping reduce the possibility of counterfeit devices accessing your infrastructure.

## BLACKBERRY 10/BES10 FIPS 140-2 CERTIFICATION

Businesses and governmental agencies alike need to feel confident that their highly sensitive data—whether it's in storage or in transit—stays secure from would-be hackers. The U.S. government created and implemented the FIPS 140-2 computer security standard, and uses it to accredit file encryption modules.

Both the BlackBerry 10 OS and BES10 software are FIPS 140-2 certified, which means that your organization's data files are strongly encrypted and can only be accessed by the appropriate encryption keys.
*See **Tech Corner 1** for more details.*

### TECH CORNER 1: FIPS 140-2 CERTIFICATION DETAILS

The FIPS 140-2 certification was implemented by the National Institute of Standards and Technology to govern cryptography modules that involve both hardware and software components.

The BlackBerry OS cryptographic kernel, which received FIPS 140-2 certification for the BlackBerry 10 OS and BES10, generates the file encryption keys, the work domain key, the work master key and the system master key to provide a strong layer of security to protect data.

The FIPS 140-2 certificate for BlackBerry 10 and BES10 are:

**BlackBerry Enterprise Service 10**
FIPS-1402 Certificate no. 1765
Consolidated Certificate no. 0019
**http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1765**

**BlackBerry 10**
FIPS 140-2 Certificate no. 1578
Consolidated Certificate no. 0007
**http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/FIPS140ConsolidatedCertList0007.pdf**

## ENCRYPTION OPTIONS

BES10 uses a technique called tunneling to help protect data in transit over the Verizon 4G LTE network. Tunneling incorporates multiple layers of encryption between devices, BES10 and the wireless resource for additional data protection.

For example, when an employee accesses the corporate Wi-Fi network, data transmissions between their device and BES10 are encrypted first by SSL encryption and then by Wi-Fi encryption.

BES10 includes additional encryption options for in-transit data security, including:

+ **Wi-Fi encryption (IEEE 802.11)**: Encrypts data transmitted between mobile devices and wireless access points set up to use Wi-Fi encryption.
+ **VPN encryption**: Encrypts data transmitted between mobile devices and VPN servers.
+ **TLS encryption**: Encrypts data transmitted between mobile devices and the BlackBerry infrastructure or BES10.
+ **SSL/TLS encryption**: Encrypts data transmitted between mobile devices and content servers, Web servers or messaging servers that use Microsoft ActiveSync.
+ **AES encryption**: Encrypts data transmissions between mobile devices and BES10.

## S/MIME MESSAGING ENCRYPTION

BES10 gives you the option of using digital certificates to sign and encrypt email and file attachments using industry standard S/MIME encryption. When IT personnel activate a mobile device on BES10, the device can be configured to sign and encrypt messages using S/MIME whenever the employee sends emails via his or her work account. S/MIME encryption keeps messages secure by using recipients' public keys to encrypt the message and their private key to decrypt it.
*See **Tech Corner 2** for more details.*

## COMMON ACCESS CARD/SMART CARD READER SUPPORT

BES10 supports BlackBerry Smart Card Readers, which allow mobile employees to use multifactor authentication with Bluetooth®-enabled BlackBerry 10 smartphones. Common Access Card (CAC) support enables two-factor authentication that grants employees access to their smartphone's work space or to the entire device itself (BlackBerry Balance). In addition, CAC has the ability to store private keys for S/MIME signing on the smart card, while also supporting the digital signing and encrypting of S/MIME emails and attachments.

## BLACKBERRY SMART CARD READER

The BlackBerry Smart Card Reader lets employees authenticate (when in proximity) with their smart cards and log into Bluetooth-enabled mobile devices. The BlackBerry Smart Card Reader functions as follows:

+ Communicates with Bluetooth-enabled BlackBerry mobile devices using Bluetooth technology version 1.1 or later, while using the AES-256 encryption method (by default) on the application layer.
+ Enables the wireless digital signing and encryption of email messages sent from BlackBerry devices using the S/MIME Support Package for BlackBerry smartphones.
+ Locks BlackBerry devices when the smart card is not in proximity.

### TECH CORNER 2: S/MIME KEYS, CERTIFICATES AND ENCRYPTION ALGORITHMS

BlackBerry devices support keys and certificates for the following file formats and file name extensions:

+ PEM (.pem, .cer)
+ DER (.der, .cer)
+ PFX (.pfx, .p12)

A private key and certificate must be stored on the device for each recipient of an encrypted email message. Keys and certificates can be stored simply by importing the files from a work email message. To send encrypted messages, your employees must use their work email accounts.

The following encryption algorithms can be used by BlackBerry devices to encrypt S/MIME-protected messages:

+ AES (256-bit)
+ AES (192-bit)
+ AES (128-bit)
+ Triple DES
+ RC2

# BES10 LAYERS OF PROTECTION

### IN-TRANSIT DATA PROTECTION
BES10 protects data transmissions using transport layer encryption and transport layer security.

### WORK DATA DEVICE PROTECTION
Work file systems and applications are kept separate from personal data and encrypted.

### PERSONAL DATA DEVICE PROTECTION
IT managers can create policy rules to encrypt data within the personal file system.

### DEVICE ACCESS CONTROL
Work Wi-Fi and VPN profiles can be delivered remotely via BES10 to enable corporate network access.

### DEVICE BEHAVIOR CONTROL
IT managers can remotely lock mobile devices, enforce policies, delete work/personal data and return devices to their default settings.

### BLACKBERRY 10 OS PROTECTION
BlackBerry devices conduct integrity tests to detect kernel damage and restart processes that stop responding.

### APPLICATION DATA PROTECTION VIA SANDBOXING
Sandboxing separates and restricts the capabilities and permissions of applications running on the device.

### RESOURCE PROTECTION
Adaptive partitioning is used to allocate unused resources during typical operating conditions, to help ensure resources are available during peak conditions.

### ACCESS CAPABILITIES PERMISSIONS MANAGEMENT
The BlackBerry 10 OS evaluates each device capability request made by an application, then grants access accordingly.

### DEVICE USER INFORMATION PROTECTION
Users can delete all their information and application data from device memory.

### BOOT ROM CODE VERIFICATION
The device verifies that the boot ROM code has permission to run on the device.

**BES10** CONTAINS MULTIPLE LAYERS OF PROTECTION, SO DATA STAYS SECURE BOTH IN TRANSIT AND ON DEVICES.

# PROTECTING DATA AT REST

## BLACKBERRY BALANCE AND BLACKBERRY ENTERPRISE SERVICE 10 HELP PROTECT SENSITIVE DATA.

PROTECTING DATA STORED ON EMPLOYEES' DEVICES FORMS A CRITICAL PART OF ANY COMPREHENSIVE MOBILE DATA SECURITY PLAN. CORPORATE DATA CONTAINED ON MOBILE DEVICES PRESENT A SIGNIFICANT TARGET OF OPPORTUNITY FOR MISUSE IF THE DEVICE IS LOST OR STOLEN. ALSO, THE WIDESPREAD USAGE OF EMPLOYEE-OWNED DEVICES IN CORPORATE ENVIRONMENTS CREATE ADDITIONAL DATA SECURITY CHALLENGES AS EMPLOYEES ACCESS BOTH WORK AND PERSONAL INFORMATION FROM THE SAME DEVICE.

With BlackBerry Balance™, a feature of BES10, you can create "dual personas" on employees' mobile devices, which separate work mobile profiles from personal mobile profiles, using independent cryptographically portioned file systems without the need for additional third-party data protection software.

BlackBerry Balance identifies and tags data that originates from your company Wi-Fi, VPN access or intranet, and routes it to the employee's work profile on the device. Other data, including third-party applications, Web browsing and personal email, is contained within their personal profile.

### BLACKBERRY BALANCE OVERVIEW AND FEATURES

BlackBerry Balance keeps employees' work and personal information separate and secure on BlackBerry 10 devices using specifically designated areas called spaces. Within each of these spaces, data, applications and network connections can be safely stored. Individual spaces can be governed by their own rules for data storage, application permissions and network routing. Using separate spaces for work and personal activities helps keep sensitive data secure by preventing employees from copying work data into personal email, or displaying information during video chats.

BlackBerry Balance lets you control how devices separate, secure and protect company data and resources. Using BlackBerry Balance, you can:

+ Control employee access to company data and applications on their devices.
+ Help prevent company data from becoming compromised.
+ Provide a unified and consistent user experience with a core set of applications when accessing personal or work data.
+ Install and manage company applications on employees' devices remotely.
+ Remove company data and applications from employees' personal devices when needed.
+ Control network connections for work and personal applications remotely.

## BUILT-IN PASSWORD PROTECTION

BES10 allows your IT personnel to establish and enforce password policies quickly and easily to better protect data stored in employees' devices. IT policies can be set to require your employees to enter a password or use their corporate single sign-on using Active Directory® services to proceed. This keeps data at rest on employee devices safe and protected.

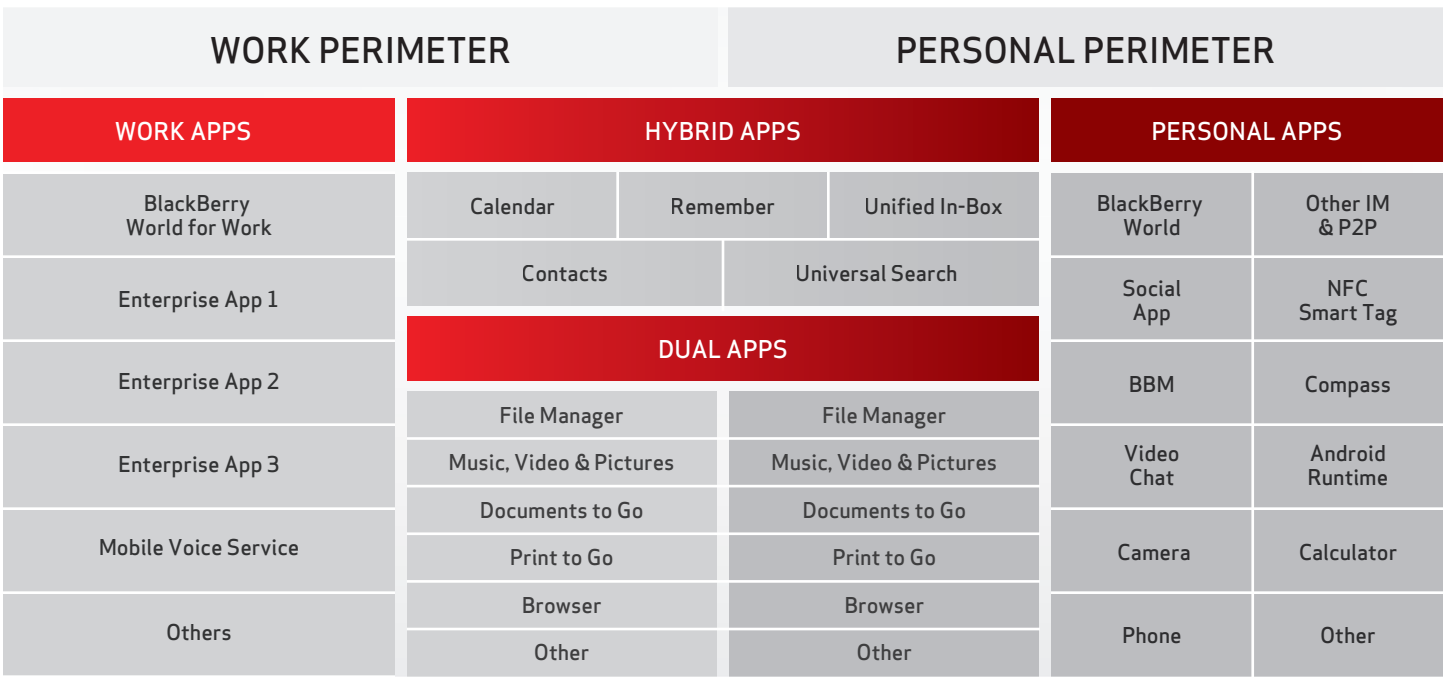
### BLACKBERRY BALANCE IN ACTION

An employee in a company's marketing department accidentally receives an email intended for someone in the finance department. The email contains information regarding future company plans that may impact shareholder value and could be used for insider trading.

The employee believes he can profit from the privileged information before the error is discovered and help a few friends out as well. He plans to forward the message to others, but realizes that it would be tracked by the company's corporate email system. He then decides to copy and paste the message into his personal email account for delivery. However, BlackBerry Balance prevents the copy-and-paste functions from working between the employee's work profile and his personal profile. As a result, the employee cannot paste the information into a personal email to bypass logging.

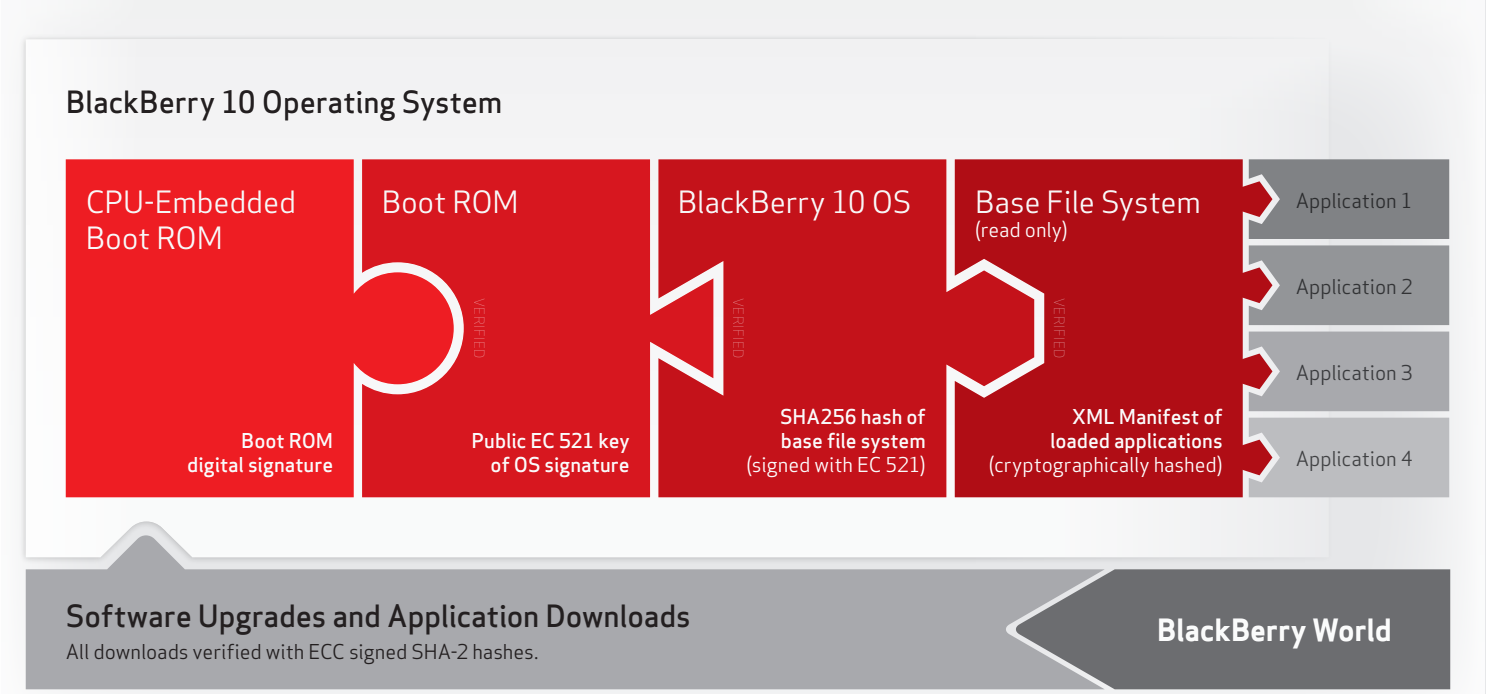
## TECH CORNER 3: WORK PERIMETERS/PERSONAL PERIMETERS IN DETAIL

BlackBerry Balance allows you to establish perimeters on employees' devices to separate work applications and data from personal applications and data, with some resources shared between the two.



# STRONG ACCESS CONTROLS

## THE BLACKBERRY SOLUTION VERIFIES THAT THE DEVICES ATTEMPTING TO CONNECT TO THE NETWORK AND ACCESS DATA ARE AUTHENTIC AND AUTHORIZED TO DO SO.




THE SOLUTION CONTAINS MULTIPLE FEATURES, SUCH AS DEVICE AUTHENTICATION, ANTI-COUNTERFEITING MANUFACTURING CONTROLS AND DEVICE OS PROTECTION, THAT VERIFY AND MAINTAIN DEVICE INTEGRITY. THESE FEATURES HELP ENSURE ONLY AUTHORIZED DEVICES USED BY AUTHORIZED EMPLOYEES GAIN ENTRY INTO YOUR NETWORK, USE NETWORK SERVICES AND ACCESS DATA.

### BLACKBERRY HARDWARE ROOT OF TRUST

BlackBerry takes specific steps to help ensure the integrity of its devices and prevent counterfeit devices from connecting to the BlackBerry infrastructure.

Security is built into each major BlackBerry device component, making it more difficult to remove or circumvent. Plus, all parts of the BlackBerry supply chain, from its manufacturing partners to the BlackBerry infrastructure and devices, are all securely connected, which means trusted BlackBerry devices can be built around the world.

This secure manufacturing model helps prevent the impersonation of authentic BlackBerry devices and ensures that only authentic BlackBerry devices can connect to its infrastructure. Any device trying to connect to the BlackBerry infrastructure must complete the self-verification process before access is granted.

## AUTHENTICATION

Multiple forms of authentication take place within the BlackBerry system to minimize the possibility of data loss and outside attack. First, the BlackBerry infrastructure and BES10 must authenticate with each other before data transmission takes place. At this level, BES10 and the BlackBerry infrastructure share a Server Routing Protocol (SRP) authentication key before a connection takes place.

The second level of authentication takes place between BES10 and the BlackBerry 10 device. When the device is activated, it generates a key pair and sends the public key to the BES10 server. The BES10 server then creates a client certificate and sends an enterprise management root certificate and client certificate back to the device. It uses the enterprise management root certificate to authenticate the server certificate for the enterprise management Web service. BES10 and the BlackBerry 10 device use the client certificate to authenticate users, their work spaces and their devices.

## BLACKBERRY DEVICE OS SECURITY FEATURES

Protecting the device's OS is one of the more important functions of mobile device security. However, it's sometimes neglected by other manufacturers, since it can be challenging to verify the security vulnerabilities contained in millions of lines of source code. The BlackBerry 10 OS includes security features for OS protection, including:

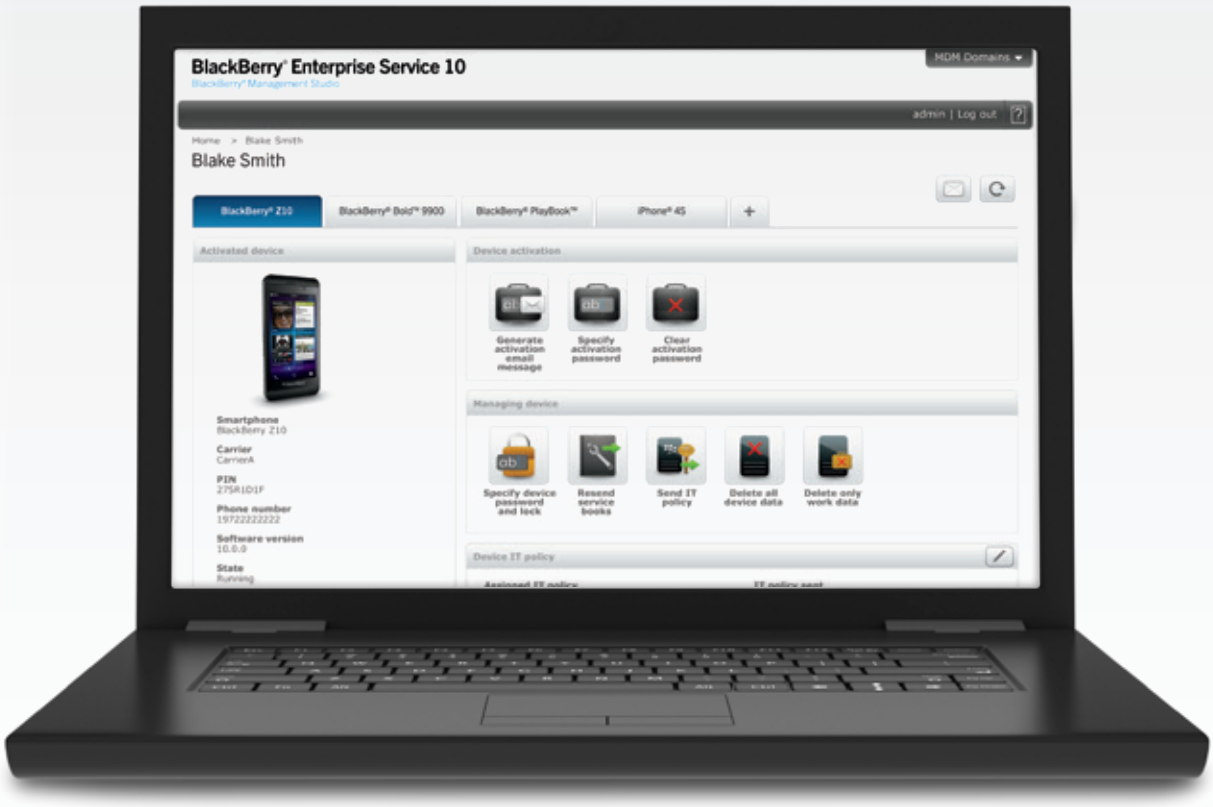
+ **Microkernel implementation:** The hardened QNX kernel used in the BlackBerry 10 OS contains approximately 150,000 lines of code. With fewer lines of code, it helps the BlackBerry OS reduce potential vulnerabilities, making it more secure. As a result, security verification and testing are more thorough, even with a fixed amount of IT resources.
+ **Resilient design:** The microkernel contains processes in the user's personal profile and any unresponsive processes are automatically restarted without impacting others.
+ **Root process minimization:** To help reduce security risks, only the most essential BlackBerry processes are run in root mode. This mode is not available to outside third parties.

## BLACKBERRY WORLD

Once a BlackBerry 10 device is activated on BES10, it has two separate BlackBerry World application storefronts: BlackBerry World, which is stored in the device's personal space, and BlackBerry World for Work, which is stored in the device's work space. Employees can download and install only the applications hosted by your company, deployed via BES10 and/or available in BlackBerry World, but are designated as optional for the work space on their devices. Any application that is not approved by your company cannot be installed into the work space. Any application downloaded from BlackBerry World is installed in the device's personal space, to further protect corporate information.

# ENTERPRISE MOBILITY

## WITH BES10, YOU CAN EASILY MANAGE BLACKBERRY, iOS AND ANDROID DEVICES FROM ONE CENTRAL LOCATION.




A TYPICAL ENTERPRISE CONTAINS POTENTIALLY THOUSANDS OF DEVICES, EACH ONE A POTENTIAL UNAUTHORIZED ENTRY POINT INTO YOUR CORPORATE NETWORK. IT'S UNFEASIBLE TO MANUALLY CONFIGURE, AUTHORIZE AND SECURE EACH DEVICE SEPARATELY. YET, WITHOUT THE PROPER TOOLS IN PLACE, MANY OF THESE DEVICES COULD SLIP THROUGH THE CRACKS AND NOT BE PROPERLY SECURED, WHICH COULD THEN BE USED TO ACCESS DATA IMPROPERLY.

BES10 offers full cross-platform mobile device management capabilities for BlackBerry, iOS and Android devices through a single administration console. BES10 allows IT administrators to control device activation, policies and settings, as well as monitor, manage and troubleshoot devices remotely over the Verizon 4G LTE network.

### BLACKBERRY 10 DEVICE ACTIVATION

During activation, a customized work space is created on the employee's BlackBerry 10 device, and it becomes associated with that specific employee within BES10. Once the device is activated, a secure communication channel is established between the device and BES10 to enable data transmission.

The BES10 also allows multiple BlackBerry 10 devices, including tablets and smartphones, to be activated for the same user account. After activation, IT administrators can send email, applications, profiles, policies and other work-related items directly to the device via the BES10 over the Verizon 4G LTE network.

### BLACKBERRY USER AUTHENTICATION IN ACTION

You've hired several new employees—each due to receive his or her own BlackBerry 10 smartphone. A member of your IT department quickly and easily adds each employee as a new user account into the BES10, using information he pulled from your company's Microsoft Active Directory. An activation password for each account is created and delivered to the respective employee.

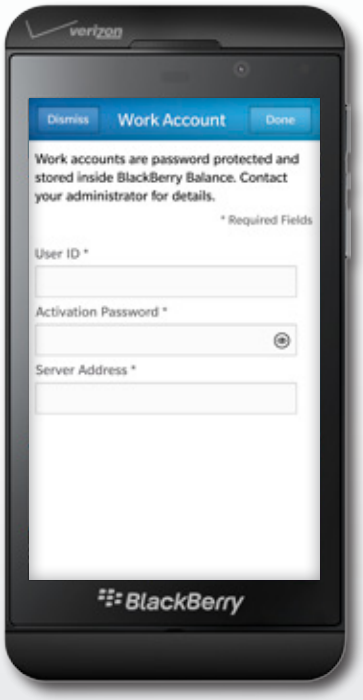
Each new employee receives a BlackBerry 10 device and the activation password from the IT department. The employees type their user IDs and passwords into the smartphones to activate them.

The smartphone's enterprise management agent automatically identifies the BES10 SRP and establishes a secure connection through the BlackBerry infrastructure over the Verizon 4G LTE network to the BES10. Encryption keys, based on your IT department policies, are generated, work spaces are created and profiles and software configurations are sent to each smartphone. They are ready to go.

## MANAGING DEVICES USING DEVICE WIPE

With BES10 and BlackBerry Balance, you can keep company data safe while leaving employee personal data intact. Using BES10, you can remotely wipe an employee's work space and all its contents from devices, leaving all personal data on the device in place.

You can also use BES10 to create policies that delete the work space from the device if certain events occur or specific conditions are met. For example, you can create a policy to delete the work space if the number of failed password attempts exceeds the maximum number allowed. You can also wipe the device if employees exceed their allotment of permitted hours or days since its last network connection.




### DEVICE WIPE IN ACTION

One of your employees has just received a job offer from a competitor. This employee works in your company's procurement department and has access to the company ERP system via her personally owned BlackBerry 10 device. Using the ERP system application, the employee can see your suppliers, vendors, parts inventory, backlogs, sales projections and more.

The employee accepted the job offer and gives you her two-week notice. You alert your HR and IT departments about her upcoming departure. On her last day, IT wipes the employee's work profile from her BlackBerry 10 device, which prevents her from accessing the ERP and email systems. However, all of her personal information remains intact on her device as she uses it at her next job. During the interim remaining two weeks, BlackBerry Balance prevents the employee from removing any corporate data accessible on the device.

## DISTRIBUTION AND APPLICATION SECURITY USING BLACKBERRY WORLD FOR WORK

One of the benefits of using BlackBerry Balance is that it allows you to create and deploy your own business application store, called BlackBerry World for Work.

With BlackBerry World for Work, you can push, install and manage business and productivity applications over the Verizon 4G LTE network to BlackBerry 10 device work spaces via BES10. Most importantly with Balance, enterprise application developers need not concern themselves with designing security into their applications because using BES10 with Balance means that security is automatically addressed. This architecture dynamic means your organization can cost effectively create and deploy secure work applications.

You can also manage applications from your personalized store on iOS and Android devices as well, empowering you to control applications across multiple platforms via the BES10 administration console.

## APPLICATION SANDBOXING

The application sandboxing, Balance and malware controls found in BlackBerry 10 help keep your company data safe and secure from potentially malicious applications. BlackBerry 10 also protects employees' personal data by allowing them to configure their devices' application controls and limit application access to their personal information.

Sandboxing separates and restricts an application's capabilities and permissions by establishing separate secure work and personal spaces. The sandbox is a virtual container that uses device memory and cryptographically partitioned files systems and grants access to the application at a specific time. Applications can have sandboxes in both an employee's work space and personal space; yet each remain isolated from each other. The BlackBerry 10 OS monitors application process requests for memory outside its sandbox. If the application attempts to access memory outside its sandbox, the BlackBerry 10 OS will stop the process and reclaim the memory it uses, then restart the process without impacting other processes operating at the same time. In addition, each application is assigned its own specific group identification, which cannot be shared or reused by another application. Each application stores data in its own sandbox and the BlackBerry 10 OS prevent other applications from accessing this specific data.

## MALWARE CONTROLS

The BlackBerry 10 OS includes tight controls and design techniques to reduce the possibility of malware attacks, including a "contain-and-constrain" design strategy that minimizes risks. Application process requests are constrained within employees' personal spaces on the device, and the BlackBerry OS microkernel prevents direct inter-process communications for controling potential issues. The microkernel also monitors memory access by the personal space and authorizes its use as needed. Any application process that attempts an unauthorized memory access request is automatically restarted or shut down, protecting your company data. In the employee's personal device space, application permissions are used to protect personal data from potential malware attacks.

### MALWARE PROTECTION IN ACTION

An employee receives an email from a friend via her BlackBerry 10 device that contains multiple attachments. She opens the email within her personal profile on the device, but doesn't know that the attachments contain malware. She didn't think to turn on and off the appropriate application permissions within her personal space, which left her device vulnerable. The malware scans the employee's device for names, phone numbers, credit card numbers or any other bits of identity information that can be stolen and misused.

All company information remains isolated and stays locked down on the device's work space, fully protected and secure.

# REGULATED COMPLIANCE

## BES10 REGULATED DELIVERS THE HIGHEST LEVEL OF SECURITY, CONTROL AND DEVICE MANAGEMENT TO REGULATED BUSINESSES AND GOVERNMENTAL AGENCIES.

BES10 REGULATED PROVIDES AN EXTRA LAYER OF CONTROL TO HELP REGULATED BUSINESSES AND GOVERNMENTAL AGENCIES STAY IN COMPLIANCE. BES10 REGULATED POLICIES AND CONTROLS GIVE IT MANAGERS THE ABILITY TO DISABLE BLACKBERRY BALANCE AND RESTRICT USE TO THE WORK PERIMETER ONLY. THIS GRANTS YOU FULL GRANULAR CONTROL OVER EMPLOYEES' DEVICE FEATURES, APPLICATIONS AND FUNCTIONALITY.

### BES10 REGULATED FEATURES AND CAPABILITIES

BES10 Regulated lets you manage precisely the types of applications, tools and features employees can access on their mobile devices for additional security and to meet compliance requirements.

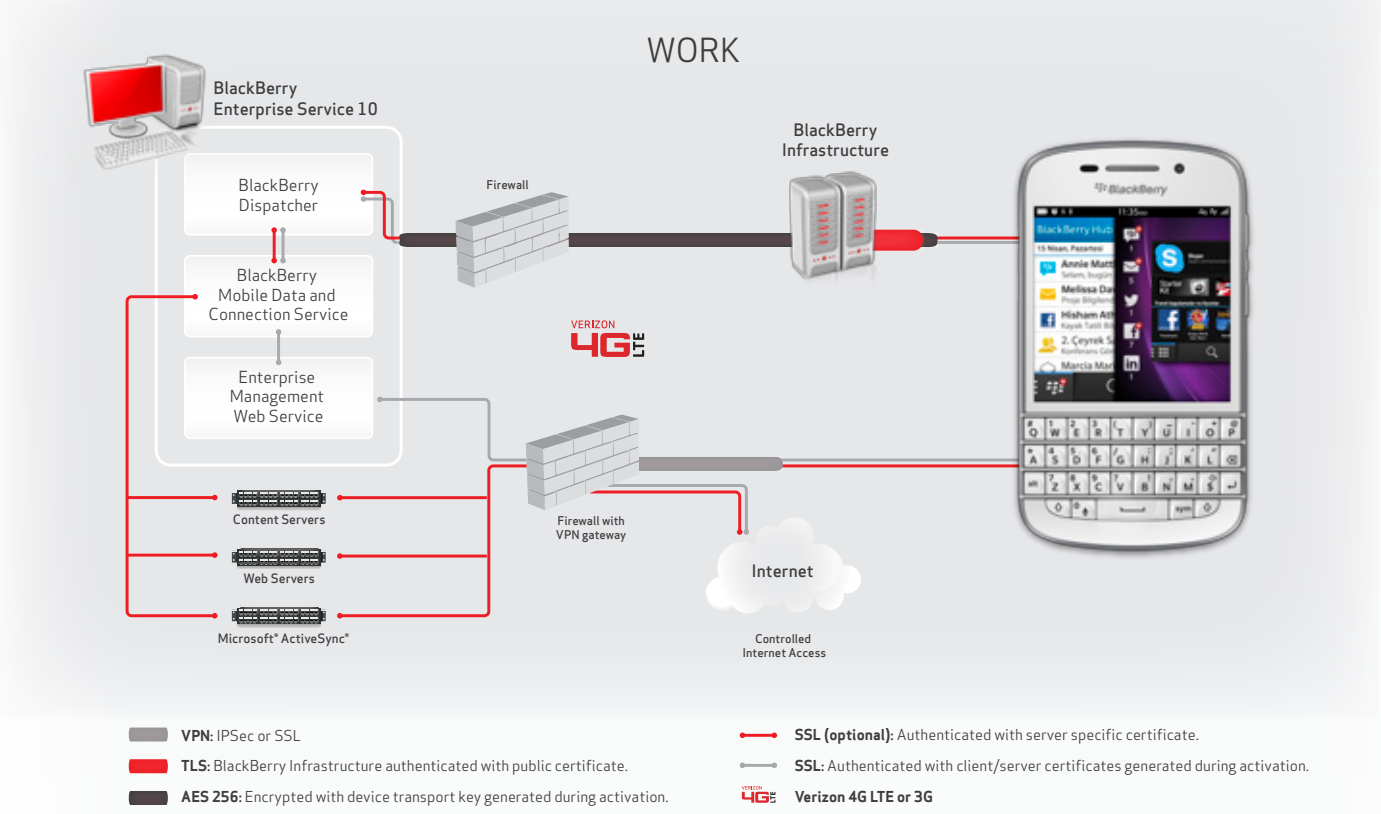
In addition to all the standard BES10 features, BES10 Regulated helps you secure your organization's data through:

+ **Communications logging:** Monitor and log all communications activities that take place on employees' BlackBerry devices with BES Regulated, including:
  - BlackBerry Messenger messages
  - Call logs
  - Pin-to-pin messages
  - SMS/MMS messages
  - Video call logs
+ **Hardware control:** Gain complete control over employees' device features and functionality by enabling or disabling:
  - Wi-Fi sharing
  - USB mass storage
  - Camera functionality
  - Video chat
  - Location-based services
  - Bluetooth connectivity
  - Near-field communications
  - High-definition multimedia interfaces
  - SD card encryption
+ **Network connectivity control:** Track and manage data as it flows through your network infrastructure, as well as the type of content employees can access through their devices. You can enable or disable:
  - Network protocols, such as SMS, MMS and BlackBerry Messenger
  - Data roaming
  - Personal information manager (PIM) accounts

BES10 also allows you to establish and deploy advanced business-to-business security policies.

*See Tech Corner 4 for more details.*

BES10 REGULATED DELIVERS ENHANCED BLACKBERRY DEVICE MANAGEMENT CAPABILITIES TO HELP GOVERNMENTAL AGENCIES AND REGULATED INDUSTRIES REMAIN COMPLIANT.




## TECH CORNER 4: BES10 REGULATED WORK PERIMETERS

BES10 Regulated allows you to approve or reject applications and tools that can be accessed by the BlackBerry 10 device.

### WORK PERIMETER

| WORK APPS | | | | | | |
|---|---|---|---|---|---|---|
| BlackBerry World for Work | Contacts | Remember | File Manager | Social App | Camera | NFC Smart Tag |
| Mobile Voice Service | Music, Video & Pictures | Universal Search | Print to Go | BBM | Calculator | Compass |
| Calendar | Browser | Documents to Go | Unified In-Box | Video Chat | Phone | Android Runtime |

# GOVERNMENT AGENCIES: SECURING DATA AND THE PUBLIC TRUST

As the general public grows accustomed to doing more with smartphones and tablets, more agencies are recognizing the urgent need to keep pace with the citizens they serve. Urged by the U.S. Digital Government Strategy,[1] government organizations are turning to mobile technology to modernize outdated systems and processes. A report[2] by Deloitte revealed that by doubling their mobile adoption rates, federal agencies could generate up to $50 billion in added value annually. In response, the Pentagon plans to roll out as many as 100,000 new mobile devices by the end of 2014.

## COST-EFFECTIVE, SECURE MOBILE TECHNOLOGIES

The mobile revolution offers government entities an opportunity to reach a new level of productivity and efficiency. But as organizations adopt new technologies, they must build the appropriate security and control measures into their systems. That means finding smarter, more affordable ways to securely manage mobile devices, applications and data.

## MOBILE SOLUTIONS THAT RESPECT PRIVATE INFORMATION AND KEEP IT IN A SAFE PLACE

### ATTAIN THE HIGHEST LEVEL OF GOVERNMENT SECURITY AND CONTROL WITH BES10 REGULATED.

BlackBerry® Enterprise Service 10 Regulated (BES10 Regulated) provides government agencies full granular control over device features, application and functionality to minimize risk, safeguard data and simplify deployment:

### ADDED SECURITY

+ **STIG-Approved**—The security technical implementation guides (STIGs) for BlackBerry 10 smartphones with BlackBerry Enterprise Service 10* are approved and supported by the Pentagon.
+ **S/MIME Encryption**—Email and file attachments are signed and encrypted using the industry standard.
+ **FIPS-140 Certification**—Highly sensitive data stored on the device is encrypted using the U.S. government computer security standard.
+ **Communication Logging**—Track and log all BlackBerry Messenger (BBM), PIN-to-PIN, SMS and MMS messages; voice calls; and video calls to meet regulatory requirements and capture data leaks.
+ **Common Access Card (CAC)/Smart Card Reader Support**—Allows mobile employees to use multifactor authentication with Bluetooth®-enabled BlackBerry 10 smartphones

### CONTROL

+ **Hardware Control**—Disable specific hardware components, including USB mass storage, camera, video, HDMI, Wi-Fi, Bluetooth and more, to meet regulation policies.
+ **Control Network Connectivity**—Track and manage employee network access and Internet usage on mobile devices.
+ **Application Management**—Deploy and manage government applications. Control use of non approved apps, including video services, social-based tools and more.

Verizon understands mobile data security is a top priority for government organizations. The right blend of mobile devices and services can help federal agencies streamline operations, cut response times, control costs and extend the reach of government employees and services beyond the office. BES10 Regulated delivers the optimal security, control and app management capabilities that agencies need to ensure compliance.

[1] Digital Government. *Building a 21st Century Platform to Better Serve the American People.*
[2] Deloitte University Press. *Gov on the go: Boosting Public Sector Productivity by Going Mobile.* February 18, 2013.

# HEALTHCARE: SECURING THE FLOW OF PROTECTED HEALTH DATA

## BES10 REGULATED DELIVERS THE HIGHEST LEVEL OF SECURITY, CONTROL AND DEVICE MANAGEMENT TO HEALTHCARE ORGANIZATIONS.

Americans are living longer and using more healthcare services. Chronic conditions like obesity and diabetes are more common—and more treatable—than ever before. We're relying on more prescriptions to help us manage many previously untreatable conditions. And we're often getting repetitive tests or unnecessary services when changing providers or seeking emergency treatment because our medical records aren't immediately available to the new doctor. Yet, spending more isn't making us healthier—or healthcare companies more efficient.

### EXPANDED ACCESS TO CARE AND VITAL DATA

Faced with soaring medical costs and increased regulatory oversight, healthcare companies are turning to technology to help them coordinate and more efficiently deliver the best care possible. Mobile technology can empower on-the-go employees—from affiliated physicians at different locations to field healthcare providers—with connectivity and access to critical information as they move between homes, offices, clinics and hospitals.

### ADDRESSING PATIENT PRIVACY AND SECURITY CONCERNS

But accessing and exchanging sensitive patient data in today's mobile environment is fraught with privacy and security concerns. In addition to addressing potential security breaches and identity theft, healthcare organizations must take appropriate steps to reduce the risk of related lawsuits. IT personnel need a secure, cost-effective way to manage devices—making sure mobile workers have access to the vital information and apps they need for optimal care delivery and productivity, while keeping that data safe.

### MOBILE SOLUTIONS THAT RESPECT PRIVATE INFORMATION AND KEEP IT IN A SAFE PLACE

#### BLACKBERRY ENTERPRISE SERVICE 10 REGULATED (BES10 REGULATED) PLACES KEY INFORMATION AND TOOLS SECURELY IN THE HANDS OF CARE TEAMS, WHILE PROTECTING SENSITIVE HEALTH DATA.

BES10 Regulated provides IT administrators full granular control over device features, application and functionality to help them stay in compliance with the Health Insurance Portability and Accountability Act (HIPAA) and other regulations.

BES10 Regulated includes these features to minimize risk, safeguard data and simplify deployment:

#### ADDED SECURITY

+ **S/MIME Encryption**—Email and file attachments are signed and encrypted using the industry standard.
+ **Communication Logging**—Track and log all BlackBerry Messenger (BBM), PIN-to-PIN, SMS and MMS messages; voice calls; and video calls to meet regulatory requirements and capture data leaks.

#### CONTROL

+ **Hardware Control**—Disable specific hardware components, including USB mass storage, camera, video, HDMI, Wi-Fi and Bluetooth® to meet regulation policies.
+ **Control Network Connectivity—**Track and manage employee network access and Internet usage on mobile devices. Ability to enforce a single browser ensures all Internet traffic flows through the organization's network, and audits employee Internet use to control content being viewed on corporate assets.
+ **Application Management**—Deploy and manage healthcare applications. Control use of non approved apps, including video services and social-based tools.

Verizon understands mobile data security is a top priority for healthcare conventions. The right blend of mobile devices and services can deliver reliable connectivity for better communication and collaboration, streamline processes for enhanced efficiency and control costs to ensure superior care. BES10 Regulated delivers the optimal security, control and app management capabilities essential to compliance.

# FINANCIAL SERVICES INDUSTRY: MOBILITY IN A HIGHLY REGULATED ENVIRONMENT

## BES10 REGULATED DELIVERS THE HIGHEST LEVEL OF SECURITY, CONTROL AND DEVICE MANAGEMENT TO BUSINESSES IN THE FINANCIAL SECTOR.

Employee demand for anytime, anywhere access to company back-end systems is driving change in the financial industry. User expectations for immediate answers and access to critical information, along with the security and control requirements of the organizations, are pushing IT delivery models to the limit.

### GOING FORWARD, SUCCESSFUL FINANCIAL SERVICES COMPANIES WILL NEED TO:

**Simplify and standardize** operations by focusing on the appropriate technology, implementing it across the organization and enforcing policies for application and endpoint management.

**Manage security risks and protect against fraud** by complying with external regulations and internal policies to protect sensitive data, and proactively addressing vulnerabilities to critical information and assets.

**Implement network connectivity control** by ensuring that data can be properly tracked and managed as it flows through the corporate network.

Verizon offers the solution that financial companies need to manage the challenges around mobile device security: BlackBerry® Enterprise Service 10 (BES10 Regulated) with BlackBerry 10 devices.

BES10 Regulated provides an extra layer of security to financial organizations to help them stay in compliance with government regulations. The platform offers full granular control over device features, applications and functionality while maintaining the overall BlackBerry 10 user experience.

## SECURITY

BES10 Regulated helps keep information private through S/MIME secure email. New logging capabilities track all data leaving the organization in order to meet regulatory requirements and capture data leaks, so immediate action can be taken. BES10 offers companies the ability to log all BlackBerry Messenger (BBM) messages; telephone calls; PIN-to-PIN, SMS and MMS messages; and video calls.

## CONTROL

Regulated policies on BES10 provide organizations with full control over hardware features on their BlackBerry 10 devices. Depending on the needs of the organization, specific features can be disabled and controlled to meet the most demanding requirements, including:

+ Workspace-only mode (BlackBerry Balance™ disabled)
+ Camera, Wi-Fi and Bluetooth®
+ Network connectivity (Wi-Fi file sharing, access points, USB mass storage and more)

Organizations can enforce the use of the corporate browser, making it easier to audit mobile Internet use by employees and control the content being viewed on corporate assets. Additional capabilities include disabling network protocols like SMS, MMS and BBM; controlling data roaming; and restricting personal PIM accounts.

## APP MANAGEMENT

With BES10 Regulated, administrators have complete control over app deployment, management and security, including the enforcement of use-restriction policies (BlackBerry World™, video chat, email, browser, social media and more).

# VERIZON AND BLACKBERRY:
# THE GOLD STANDARD FOR DATA PROTECTION

The combined Verizon-BlackBerry 10 security solution provides the necessary tools and capabilities your organization needs for end-to-end data protection. Using the solution, your IT managers can take proactive steps to secure data and help prevent loss or alteration. BlackBerry 10 includes user and device authentication functionality that sets the standard in mobile security and data protection. IT personnel can also keep employees' work and personal accounts separate with the BlackBerry Balance feature to help reduce potential breaches. BES10 Regulated allows IT personnel to create work space-only environments on employee devices, which adds an extra layer of security and control. Plus, using BlackBerry's device management capabilities, they can wipe or lock devices to help prevent data loss or misuse. And the built-in security features found in the BlackBerry 10 OS and the Verizon 4G LTE network helps protect data in transit from devices to your infrastructure and back again.

TO LEARN MORE ABOUT THE **BLACKBERRY 10** AND ITS SECURITY FEATURES, CONTACT YOUR VERIZON WIRELESS BUSINESS SPECIALIST, OR VISIT US AT VERIZONWIRELESS.COM/CONTACTREP.

BBSECPDF0413

4G LTE is available in more than 480 markets in the U.S.
Network details & coverage maps at **vzw.com**. © 2013 Verizon Wireless.

verizon